Положение об использовании системы DLP в соответствии с Регламентом GDPR

г. Москва

2020

1. Общие положения

1.1. Положение об использовании системы DLP в соответствии с Регламентом GDPR (далее - Положение) регламентирует процесс деятельности Компании, попадающие под Регламент GDPR.

1.2. Целью данного Положения является регламентирование деятельности работников, имеющих доступ к персональным данным, обрабатываемым в Компании.

1.3. Регламентированные в Положении пункты должны решать следующие задачи:

- предотвращение утечки персональных данных;
- соответствие работы DLP-системы требованиям Регламента GDPR;
- обработка и хранение персональных данных.

1.4. Настоящее Положение распространяется на работников следующих подразделений:

- Отдел информационных технологий;
- Отдел кадров и подразделение HR;
- Отдел информационной безопасности.

1.5.**Термины и определения:**

Защищаемая информация – информация, относящаяся к персональным данным, к коммерческой тайне или к другой информации ограниченного доступа.

Персональные данные (в соответствии с Регламентом GDPR) — любая информация о человеке, по которой он идентифицируется: пол, возраст, место жительства, умственная, культурная, экономическая, социальная идентичность.

1.6.**Принятые сокращения:**

ИБ - Информационная безопасность

ПДн - Персональные данные

РФ - Российская федерация

ФЗ - Федеральный закон

DLP - Data Leak Prevention (система предотвращения утечек информации)

GDPR - General Data Protection Regulation

2. Правовые и нормативно-методические источники

Настоящее Положение разработано в соответствии со следующими нормативными правовыми актами:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- General Data Protection Regulation, GDPR.

3. Защита персональных данных в соответствии с Регламентом GDPR

3.1. Регламент GDPR является законодательной базой по защите ПДн граждан Европейского Союза, с помощью которого Европейский парламент, Совет Европейского Союза и Европейская комиссия усиливают и унифицируют защиту персональных данных всех лиц в Европейском Союзе (далее - ЕС).

3.2. Ключевые принципы GDPR при обработке персональных данных:

- Законность, справедливость и прозрачность — должны быть легальные основания в рамках GDPR для сбора и использования данных, ненарушение любых законов, открытость, честность от начала и до конца об использовании персональных данных;
- Ограничение целью — обработка должна сводиться к тому, что было заявлено субъекту данных. Все конкретные задачи должны быть закреплены в политике приватности и должны чётко соблюдаться;
- Минимизация данных — использование адекватного количества данных для выполнения поставленных целей, ограниченных только необходимым количеством;
- Точность — персональные данные должны быть точными и не должны вводить в заблуждение; исправление неправильных;
- Ограничение хранения данных — не хранить данные дольше, чем нужно, периодически проводить аудит данных и удалять неиспользуемые;
- Целостность и конфиденциальность/безопасность — хранить данные в безопасном месте и уделять достаточное внимание сохранности данных;
- Подотчётность — ответственность за обработку персональных данных и выполнение всех остальных принципов GDPR, включая записи о конфиденциальности; защите, использовании, проверки данных; назначении должностного лица по защите данных (DPO, data protection officer).

4. Обработка персональных данных в системе DLP

4.1. Под действие Регламента GDPR попадает полностью или частично автоматизированная обработка персональных данных граждан ЕС на территории Европейского Союза и за его пределами физическими или юридическими лицами, государственными органами и другими институтами, и организациями.

4.2. Любая, даже некоммерческая, деятельность, связанная с обработкой персональных данных, попадает под действие GDPR.

4.3. DLP-система обрабатывает и анализирует ПДн сотрудников Компании как в ручном, так и в автоматическом режиме. В соответствии с требованиями Регламента GDPR, Компания обязуется защищать персональных данных сотрудников, обрабатываемые посредством DLP-системы.

4.4. Администраторы DLP-системы оповещаются о том, что в рамках своих должностных обязанностей они обрабатывают ПДн сотрудников.

4.5. Администраторам DLP-системы запрещено:

- разглашать и передавать третьим лицам ПДн, доверенные им в рамках их должностных обязанностей;
- использовать ПДн, доверенные им в рамках их должностных обязанностей, в личных или корыстных целях.

4.6. Для обеспечения конфиденциальности ПДн доступ к событиям, содержащим ПДн работников Компании, разграничен в соответствии с должностными обязанностями Администраторов DLP-системы.

4.7. При обработке событий DLP-системы и обработке ПДн работников, Администраторами DLP-системы реализуется принцип «четырех глаз» для обеспечения корректной обработки ПДн и дополнительной проверки.

4.8. Администраторами DLP-системы до начала работы с DLP-системой подписывается соглашение о неразглашении ПДн.

5. Ответственность

5.1. Администраторы DLP-системы несут ответственность за обеспечение конфиденциальности и сохранности ПДн, доверенных им в рамках должностных обязанностей.

5.2. Компания обязуется не использовать программные (программно-аппаратные) средства контроля за использованием технических средств с целью умышленного тайного сбора личной информации работников Компании.

6. Заключительные положения

6.1. Настоящее Положение является локально-нормативным актом Компании.

6.2. Актуализация настоящего Положения должна быть осуществлена в любом из следующих случаев:

- при изменении законодательства Российской Федерации в области защиты информации;
- при изменении требований Регламента GDPR;
- по решению руководства Компании;
- при изменении целей / средств контроля использования технических средств;
- при изменении организационной структуры;
- при появлении необходимости в изменении процесса контроля использования технических средств.

6.3. Ознакомление работников Компании с требованиями настоящего Положения осуществляется работниками отдела информационной безопасности.

6.4. Контроль исполнения требований настоящего Положения осуществляется руководителем отдела информационной безопасности.